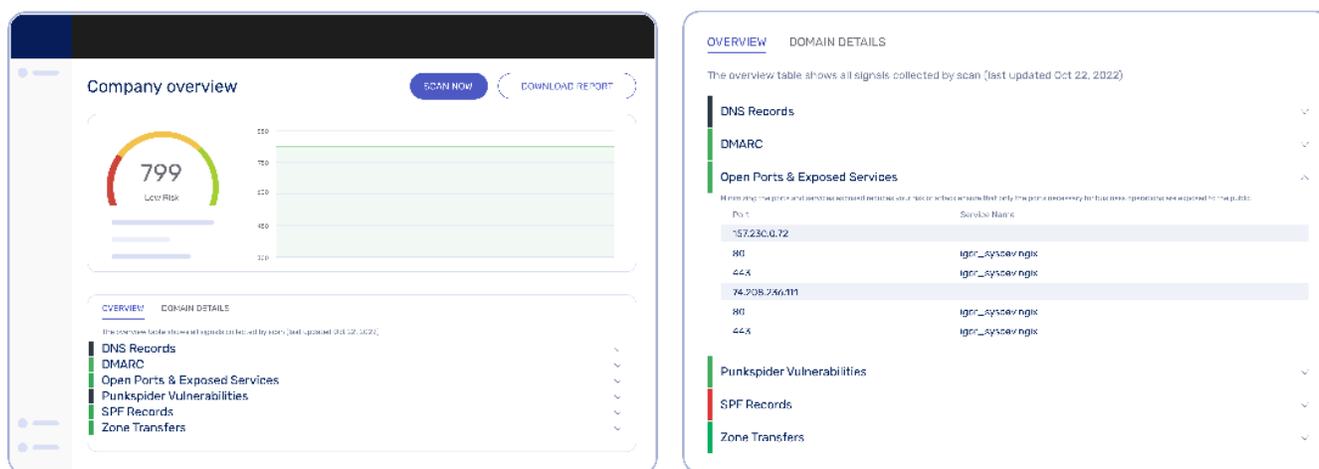


Q:SCAN

Score your external security posture



Present the very best version of yourself to the internet

Your organization uses the internet to conduct all kinds of business. You have public websites, email servers, infrastructure, and business applications, running in your own data centers, in the cloud, and on partner platforms. You have people—lots of people—working in their professional capacities but also living their lives outside of work. This unique mix of public and private resources all produce signals that attackers seek to understand and exploit, and that customers use to judge the health of your security program.

Nothing invites theft like a broken window. How you appear to others sends powerful signals about how you should be treated. With internet security as with life, appearances matter. And the consequences can be severe: cyber criminals are continually seeking to steal data, damage reputations, and extort ransoms. But even the most opportunistic digital thief knows basic economics: rattle doorknobs to find houses to rob. Look for signals that suggest poor habits. Survey targets to find the easiest ways in.

Solution

Q:SCAN is a new way for your cybersecurity team to see your organization's security the way an attacker sees it. Q:SCAN was developed in collaboration with our Offensive Security group to focus on data collection and analysis techniques of high-risk signals that are valuable to attackers. Q:SCAN can be used all by itself, or it can complement the vulnerability scanning tools you are already using.

Q:SCAN actively scans internet domains and IP ranges to identify key risk signals that can indicate your organization may have poor security posture. To accomplish this Q:SCAN collects a wide range of data such as exposed services, vulnerabilities, and validation of SSL certificates. Additionally, Q:SCAN employs a collection of unique tools built by QOMPLX such as our mass web vulnerability scanner Punkspider. By monitoring such a board range of signals Q:SCAN is capable of accurately assessing the risk posed by an organizations external attack surface.

Q:SCAN allows users to add not only domains, but IP address and companies as well. We have developed a large dataset of companies and the assets they own so our users don't have to. By organizing assets into Q:SCAN portfolios, users may monitor not only what they own themselves, but also third party vendors, M&A targets, clients, or anything else. Assets in each portfolio are evaluated and scored individually, but also grouped together with an overall risk score. This allows users to quickly identify areas of high risk and keeps them armed with up to date information. To help you take action, QOMPLX experts are available to provide guidance and recommendations whenever you need it.

Benefits

Today	With Q:SCAN
Attackers see your organization and the risk posed by your vendors.	Q:SCAN analyzes high-risk signals that attackers may seek to exploit. You have complete control over which domains or companies to monitor.
Your vulnerability scanning tools don't give you the full picture.	Q:SCAN looks at a wide range of public and proprietary datasets to provide advanced analytics that identify whether your company or its employees have been cited in breaches, cyber events or IP address reputation lists.
You spend too much time fending off questions from customers about your security program.	Q:SCAN helps you get ahead of customers' third-party risk management teams by identifying external weaknesses, reducing the time and money your staff needs to spend on inquiries.
Your organization's reputation is damaged by third-party reports that attribute risks to assets you do not own.	Q:SCAN offers an accurate analysis of your internet-facing presence by scanning assets linked to your domain. Q:SCAN does not guess what assets "might" belong to your organization.

Key Features

Q:SCAN's key features include:

- **Detailed risk exposure alerts.** Q:SCAN alerts you on external exposures including data breach citations, presence on IP reputation lists, observed malware databases, externally observable vulnerabilities and exposed ports.
- **On-going risk assessment and trend analysis.** Q:SCAN provides high-resolution visualization of your organization's external security posture. Reports run on a weekly basis so you always have the most up to date information.
- **Granular access control management.** Q:SCAN's role-based access control (RBAC) secures access to configurations and scan data, and optionally integrates with your organization's Single-Sign-On (SSO) system via SAML 2.0.
- **Attack Surface Monitoring.** By using Q:SCAN's portfolio features you can monitor any domain, company, or IP address, and keep them grouped however you like. Discover, monitor, and report on anything that is part of your risk profile.



Start a free 30-day trial today! Contact us.

info@QOMPLX.com | qomplx.com

Why QOMPLX®

QOMPLX harnesses data to provide unified visibility into cyber risks and trust in identity. QOMPLX solutions reduce cyber risk and attack surfaces by mapping exposures and performing real-time detection of attacks. This approach increases network observability by closing the largest remaining gaps in cybersecurity: identity verification, cross-tool data fusion, and data interoperability. QOMPLX defends some of the world's most renowned brands by re-establishing trust for client organizations, assuring authentication, and enabling confident security decisions.

For more information, visit qomplx.com and follow us [@QOMPLX](https://twitter.com/QOMPLX).